

How to Configure WAN GroupVPN on the NetVanta 2000 Series to connect using Global VPN Client

This document is applicable to NetVanta 2600 series, 2700 series, and 2800 series units.

Feature/Application:

NØTE

The NetVanta 2000 Series has the functionality to allow remote users to connect to the network behind the NetVanta 2000 Series using Global VPN Client software using IPSEC VPN protocol. This article focuses on the configuration of WAN Group VPN settings on the NetVanta 2000 Series appliance so that a remote computer can access the corporate network behind the NetVanta 2000 Series using the **Public IP 1.1.1.50**



Deployment steps:

To configure the NetVanta 2000 Series to accept GVC connections three steps have to be performed. These steps can be achieved either by following the wizard or manually.

Step 1: Configure WAN GroupVPN on the NetVanta 2000 Series appliance (In this section we will select the Encryption, authentication options and GVC client settings).

Step 2: Configure DHCP over VPN on the NetVanta 2000 Series appliance (In this section we will configure NetVanta 2000 Series to assign virtual IP addresses to GVC software).

Step 3: Configure User accounts on the NetVanta 2000 Series appliance (In this section we will create user accounts for GVC users and also Add subnets or IP addresses that the GVC users need to access.)

Step 4: How to Test

Procedure:

Step 1: Configure WAN group VPN on the NetVanta 2000 Series appliance.

To configure the WAN GroupVPN, follow these steps:

1. Login to the NetVanta 2000 Series Management Interface; go to VPN > Settings page.

2. Make sure that the Enable VPN and WAN GroupVPN check boxes are enabled:

• 🚽 System • 💇 Network • 💿 3G/Modem	vpv/ Settings			
 → SonicPoint → Firewall → O VoIP → Application Firewall >> Anti-Spam 	Accept Cancel VPN Global Settings Enable VPN			
Kongeneration Kongene	Unique Firewall Identifier: VPN Policies Start Tal	ble Refresh 🕪 Refresh Interval (secs) 10	Items per page 50 Items	Lick on the
L2TP Server	🗌 # Name Gateway De	stinations Crypto Suite	Enable	Configure
Users	1 WAN GroupVPN	ESP: 3DES/HMAC SHA (IKE)	A1	003
High Availability Security Services	2 WLAN GroupVPN	ESP: 3DES/HMAC SHA (IKE)	A1	
Log	Add., Delete			Delete All

3. Click the configure icon for the WAN GroupVPN entry. The VPN Policy window is displayed

4. In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. Enter a shared secret in the **Shared Secret** Field.

General	Proposals	Advanced	Client
Security Policy			
Authentication Method	: IKE using	g Preshared Secre	t 🗸
Name:	WAN Gro	oupVPN	
Shared Secret:	adtrantes	t	

5.Click the **Proposals** tab, use the **default settings** or choose the desired Encryption and Authentication options.

IKE (Phase 1) Proposal				
DH Group : Group 2	Polecied by ServiciALL	ork Security Appliance		
Encryption : 3DES	General	Proposals	Advanced	Client
Authentication : SHA1	Conorda	Topoodio	Addition	Chich
Life Time (seconds) : 28800				1
Ipsec (Phase 2) Proposal	IKE (Phase 1)	proposal		
Phase 2	DH Group:		Group 2	*
Protocol : ESP	Encryption:		3DES	~
Encryption : 3DES	Authentication:		SHA1	*
Authentication : SUA 1	Life Time (seconds):		28800	
Life Time (seconds) + 2000	Ipsec (Phase 2) Proposal		
Charles in the form	Protocol:	[ESP	~
Forward Secrecy if you want	Encryption:	[3DES	~
an additional Diffie-Hellman	Authentication:		SHA1	~
layer of security. Select Group	Enable Perfect	Forward Secrecy		
2 from the DH Group menu.	Life Time (seconds):		28800	
L2TP client and Windows XP				
L2TP client can only work with DH Group 2. They are	Ready			
incompatible with DH Groups 1 and 5.	OK	Ca	ancel He	lp

6.Click the **Advanced** tab.

Enable Windows Networking (NetBIOS) broadcast -	Network Security Appliance
Allows access to remote network resources by browsing	General Proposals Advanced Client
the Windows® Network Neighborhood.	Advanced Settings
Require Authentication of VPN Clients via XAUTH - So that all the users connecting	Enable Windows Networking (NetBIOS) Broadcast Enable Multicast Management via this SA: HTTP HTTPS SSH Default Gateway: 0.0.0.0
are authenticated. Unauthenticated traffic will not be allowed	Client Authentication Require authentication of VPN clients by XAUTH User group for XAUTH users:
on to connect. The Trusted users group is selected by default.	Allow Unauthenticated VPN Client Access:Select Local Network
Management via this SA: - Optionally, if you want the Remote	OK Cancel Help
users to manage the NetVanta 2000 Series security appliance,	
select the management method, either HTTP or HTTPS.	

7.Click the Client tab, select the following settings.

Cache XAUTH User Name and Password on Client : Single session	ADRAN N	letwork Security Appliance	0	
Virtual Adapter Settings: DHCP Lease	General	Proposals	Advanced	Client
Allow Connections to: Split Tunnels	User Name an	d Password Cac	hing	
Set Default Route as this Gateway: Disable	Cache XAUTH User	Name and Password	on Client: Single	Session 💌
Use Default Key for Simple Client Provisioning: Disable	Virtual Adapter sett Allow Connections 1	ings: :o:	DHCP Split T	Lease 👻 unnels 💙
	Set Default Ro	ute as this Gateway		
	Client Initial P	rovisioning	Optio box w users	nal: Checking this vill not prompt GVC s for preshared key
	Use Default Ke	y for Simple Client Pro	ovisioning	
	Ready	ОК	Cancel	Help

8. Click OK

Step 2: Configure DHCP over VPN.

To configure **DHCP over VPN** for the Central Gateway, use the following steps:

- 1. Select VPN > DHCP over VPN, select Central Gateway from the menu.
- 2. Click Configure. The DHCP over VPN Configuration window is displayed

Application Pirewall Application Pirewall Anti-Spam O VPN Settings Advanced	Cancel DHCP over VPN
DHCP over VPN L2TP Server SSLVPN Users	Central Gateway Configure

3. Select **Use Internal DHCP Server** if the NetVanta 2000 Series is the DHCP server.Check the For Global VPN Client checkbox to use the DHCP Server for Global VPN Clients.

If you want to send DHCP		
requests to specific servers,	ADRAN Network Security A	Appliance
select Send DHCP requests	Providence of Conference.	Enable this option if the
to the server addresses listed		SonicWALL appliance
below.	рнср кејау	Is the Driver server.
Click Add.	Use Internal DHCP Server	Enable this option if the DHCP server is on the
Type the IP addresses of	For Remote Firewall	to enter the Server's IP.
DHCP servers in the IP	Sand DHCB requests to the s	
Address field.	D Send DHCP requests to the s	erver addresses iisted below
	IP Address	
Click OK .		
The NetVanta 2000 Series security appliance now directs DHCP requests to the	Add Edit	Delete All
specified servers.	Relay IP Address (Optional): 0.0.	0.0
	Ready	
		OK Cancel Help

Step 3: Configure User Accounts

To configure User accounts, use the following steps:

1. Select Users > Local Users

🕶 🚇 Users	Users /
Status	Local Users
Settings	
Local Users	Local Users I to 1 (of 1)
Local Groups Guest Services	□ ► # Name CFS Policy Guest Services Admin VPN Access Configure
Guest Accounts	□ ▶ 1 All LDAP Users 🗭 🖉 🖉
Guest Status Figh Availability Geourity Services	Add User Delete All Delete All

2. Click on Add User

3. Under the settings tab give the desired name and password

Seurigs	Groups	VPN Access
ser Settings		
lame:	testuser	
Password:	•••••	
Confirm Password:	•••••	
	User must char	nge password

- 4. Go to the Groups Tab, user should be member of trusted users.
- 5. Go to VPN access tab, select the subnet that the user need to access.

Example: If you want GVC users to access VPN networks, add them to Access List section.

Settings	Groups	VPN Access	
N Client Access	Networks	Add any othe or IP addres the GVC use to access.	er subnet ses that rs need
Networks:		Access List:	
Default SonicPo Default SonicPo Default Trusted DMZ Interface II Firewalled Subr	bint ACL Allow Gro bint ACL Deny Gro Relay Agent List P nets	DMZ Subnets	//
	~	<- Remo	/e All

6. Click OK

Step 4: How to Test: Using GVC software installed on the remote computer to connect to the corporate network.

- **1.** Install the latest GVC software on the remote user's computer
- **2.** Launch the Global VPN Client software
- 3. Click on File > New Connection and click Next

Glob	oal VPN Client			
⁼ile	View Help			
#	Enable	Ctrl+B	1 2	
à	Status	Ctrl+T	er	🛆 🛛 Status
P	New Connection	Ctrl+N		
Z	Import Connection	Ctrl+I		
	Create Shortcut	•		
×	Delete	Del		
le	Rename			
P	Properties			
	Close	Alt+F4		

4. Select **Remote access** and click **Next**

w Con	nection Wizard		
Choos To be	e Scenario add a new connecti using this connection	on you must choose the scenario that best fits how y 1.	ou will
¢	Remote Access	<u>View Scenario</u>	
	Choose this scenario common use of this access the corporat	if you want to secure access to a remote firewall. T scenario is when you are at home or on the road and e network.	he most I want to
C	Office Gateway	View Scenario	
	Choose this scenari common use of this Secure Wireless pro) if you want to secure access to a local firewall. The scenario is for securing a wireless connection to an A duct.	e most ADTRAN
То	continue, click Next		
1.5			
		< Back Next >	Cancel

5. Under IP address enter the WAN / X1 IP of the NetVanta 2000 Series , click Next and click Finish

New Connection Wizard	×
Remote Access To use the remote access scena address.	rio, specify the gateway's domain name or IP
Specify the domain name or IP a	ddress of the security gateway.
IP Address or Domain Name:	1.1.30
You may also specify a name for	this connection.
Connection Name: 1	1.1.50
To continue, click Next.	
	<back next=""> Cancel</back>

6. Right click on the new connection that is created and click **Enable**

Global VPN Client					X
File View Help					
🖻 🕹 🔕 🗙 ě 😭 🖌	1				
Name	Peer		1	Status	
 1.1.1.50	1.1.1.50	TO T	to do do do do do do do do do	Disabled	
	4	Enable	Ctrl+B		
	ß	Status	Ctrl+T		
		Create Sh	ortcut 🕨		
	×	Delete	Del		
	aje	Rename			
		Properties	;		

7. Enter the **preshared secret** for the connection

Global VPN Cli	ent	_ 🗆 🗙
File View Help	8	
Name → 1.1.1.50	1.1.1.50 Image: Constraint of the pre-shared key for this connection appears to be incorrect. Enter the pre-shared key for this connection as specified by your network administrator. Pre-Shared Key: adtrantest Image: Only this contract of the pre-shared key	

8. Enter the username and password for the connection

Global VPN C	lient	
File View He	1.1.1.50	
Name	Enter Username / Password This peer requires that you log in with a username and password.	icating
	Please enter your username and password assigned to you by your network administrator. Username: testuser Password: ************************************	
	OK Cancel	

9. After entering the **username** and **password**, the adapter will try to acquire an IP address and then change to **Connected** status.

Global VPN Client			
File View Help			
🖻 ≱ 🗟 🗆 🔆 🔮 🖻	′ 🗐 🔍		
Name	Peer	Ā	Status
9 1.1.1.50	1.1.1.50		Connected

10. To check the **IP** address for the NetVanta 2000 Series virtual adapter, go to the command prompt on the computer and type the command **IPCONFIG**

